UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/583,051	06/14/2006	Peng Zhang	42P22776	8821

8791 7590 08/18/2010

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
08/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/583,051	ZHANG, PENG	
	Examiner	Art Unit	
	CARL COLIN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In communications filed on 7/20/2010, applicant amends claims 11-12. The following claims 1-20 are presented for examination.

2. In response to communications filed on 7/20/2010, the claim objection of claim 11 and the 101 rejection of claims 12-14 have been withdrawn with respect to the amendment.

3. Applicant's arguments with respect to claims 1-20 have been considered but they are not persuasive. Regarding claims 1, 7, and 12, Applicant argues that Swimmer does not disclose a virtual machine. Examiner respectfully disagrees because the claims merely recite intended use of a virtual machine. In response to applicant's argument that the prior art does not recite a virtual environment, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In addition, a virtual machine is a software that mimics the performance of a hardware device or a software implementation of a machine that executes programs like a physical machine. As the program daemon runs in the background, it creates a virtual environment for interacting with the host platform which meets the claim limitation. Examiner notes that Altman et al explicitly discloses the use of a virtual machine. Therefore, for at least the reasons above, applicant has not overcome the rejection of claims 1-20.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-3, 7-8, 11-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Swimmer et al. (US Pub. 20040255163 A1).

6. Regarding claim 1, Swimmer discloses a method comprising: receiving in a virtual machine contents of a program for creating a virtual environment for interacting with a host platform in a computing device **(para. 17, 22, 44-45; With the intrusion detection system performing the function of a virtual machine, a daemon is analogous to a program creating a virtual environment and the operating system being analogous to the host platform)**; and determining by the virtual machine if the received contents comprises predetermined instructions for performing at least one unauthorized task. **(para. 22-23- malicious code strings being analogous to predetermined instructions for performing unauthorized tasks)**

7. Regarding claim 2, Swimmer discloses the method of claim 1, wherein the determining if the received contents comprises predetermined instructions further comprises: comparing the received contents of the program to at least one predetermined instruction patterns corresponding to the predetermined instructions for performing the at least one unauthorized task **(para. 22, a pattern filter is used to identify malicious code strings)**; and purging the predetermined

instructions from the received contents based on the comparing. **(para. 15, 17- the malicious code string is extracted from the daemon code)**

8. Regarding claim 3, Swimmer discloses the method of claim 2, wherein the comparing the contents of the received program to at least one predetermined instruction patterns further comprises: searching predetermined locations of the received contents of the program for the predetermined instructions. **(para. 27, 55, 58, the memory location containing a possible infected dameon is scanned)**

9. Regarding claim 7, Swimmer discloses a system comprising: a virtual machine to receive contents of a program for creating a virtual environment for interacting with a host platform in a computing device **(para. 17, 22, 44-45; With the intrusion detection system performing the function of a virtual machine, a daemon is analogous to a program creating a virtual environment and the operating system being analogous to the host platform)**, the virtual machine comprising a detector subsystem to determine if the received contents comprises predetermined instructions for performing at least one unauthorized task. **(para. 22-23- malicious code strings being analogous to predetermined instructions for performing unauthorized tasks)**

10. Regarding claim 8, Swimmer discloses the system of claim 7, wherein the detector subsystem is to purge the predetermined instructions from the received contents of the program, wherein the detector subsystem further comprises :a comparator logic to compare the received contents of the program to at least one predetermined instruction patterns corresponding to the predetermined instructions for performing the at least one unauthorized task **(para. 22, a pattern**

filter is used to identify malicious code strings); and a search logic to search predetermined locations of the received contents of the program for the predetermined instructions. **(para. 15, 17- the malicious code string is extracted from the daemon code)**

11. Regarding claim 11, Swimmer discloses the method of claim 8, wherein the at least one predetermined instruction patterns are stored in a database in communication with the virtual machine. **(Fig. 2, element 21, para. 60-61)**

12. Regarding claims 12-14, they merely recite a computer program that when executed, performs the functional steps of method claims 1-3, and thus, rejected for the same rationale.

13. Regarding claim 15, Swimmer discloses a method comprising: receiving a system call for a host platform in communication with a virtual machine of a computing device **(para. 17- system calls are monitored)**; and determining by the virtual machine if the received system call comprises at least one predetermined system call for performing at least one unauthorized task. **(para. 17- system call patterns examined for non-normal behavior)**

14. Regarding claim 16, Swimmer discloses the method of claim 15, wherein the determining if the received system call comprises predetermined system call further comprises: comparing the system call to at least one predetermined system call patterns corresponding to the predetermined system calls for performing the at least one unauthorized task. **(para. 17)**

15. Regarding claim 17, Swimmer discloses the method of claim 16, wherein the unauthorized task comprises: a task predetermined to be an inhibitive task by the computing device; and a task to output data into memory regions storing at least one of instructions and data for operations of the virtual machine. **(para. 52- eg. The malicious code string being instructions to jump to code which 'spawns a shell' program)**

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Swimmer as applied to claim 2 above, and further in view of Altman et al. (US Pub. 20040044880 A1).

18. Regarding claim 4, Swimmer discloses the method of claim 2, but is silent on the program to be examined for unauthorized instructions residing in a translation cache and checking branch targets as recited in claim 4. However, Altman discloses a virtual machine manager which translates a portion of the virtual machine code and stored in a translation cache. **(para. 28-31)** In addition, Altman discloses checking whether a branch within the translated code branches outside to untranslated code. **(Fig. 1, para. 33)** Therefore, taking the combined teachings of Swimmer and Altman as a whole, it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize a translation cache for storing and checking the program contents for unauthorized code since it allows for faster future use of the code.

19. Regarding claim 5, the combination of Swimmer and Altman discloses the method of claim 4, further comprising: generating checking and determining instructions for performing the checking the branch target and determining if the checked branch target comprises at least one of

a translation cache and the execution engine. **(Altman- para. 28- 31, interpretation and compilation instructions)**

20. Regarding claim 6, the combination of Swimmer and Altman discloses the method of claim 2, wherein the virtual machine comprises an execution engine and at least one interpret function invoked by the execution engine, wherein the contents of the program reside in the at least one interpret function. **(Altman- para. 28-32, 38)**

21. Regarding claims 9-10, they are rejected as applied to claims 4-6 because a corresponding system would have been necessitated to carry forth the method steps of claims 4-6. The applied prior art also discloses the corresponding architecture.

22. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Swimmer further in view of Draves (US 5,873,124).

23. Regarding claim 18, Swimmer discloses a method comprising: receiving a virtualized memory address for a host platform in communication with a virtual machine of a computing device; and determining by the virtual machine if the received virtualized memory address comprises at least one predetermined unauthorized virtualized memory address. **(para. 17, 45).** However, Swimmer is silent on explicitly utilizing virtualized memory address. However, virtualized memory addresses are notoriously well known and used in the art as evidenced by Draves **(see abstract).** Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize it in the teachings of Swimmer to allow program code to be compiled as though each process will enjoy exclusive access to the entire memory address space.

24. Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Swimmer and Draves as applied to claim 18 above, and further in view of Altman et al. (US Pub. 20040044880 A1).

25. Regarding claim 19, the combination of Swimmer and Draves discloses the method of claim 18, but is silent on the virtual machine further comprising at least one of a translation cache to store translation data; an execution engine; and at least one interpret function invoked by the execution engine. However, Altman discloses a virtual machine manager which translates a portion of the virtual machine code and stored in a translation cache. **(para. 28-31).** In addition, Altman discloses an execution engine and at least one interpret function invoked by the execution engine **(para. 28-32, 38)** Therefore, taking the combined teachings of Swimmer, Draves and Altman as a whole, it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize a translation cache for storing and checking the program contents for unauthorized code since it allows for faster future use of the code.

26. Regarding claim 20, the combination of Swimmer, Draves and Altman discloses the method of claim 19, wherein the determining by the virtual machine if the received virtualized memory address comprises at least one predetermined unauthorized virtualized memory address comprises: determining if the virtualized memory address is in a memory space available to the translation cache **(Altman- para. 28-32)**; determining if the virtualized memory address is in a memory space available to the at least one interpret function **(Altman- para. 28-32)**; and determining if the virtualized memory address is in a memory space region storing at least one of instructions and data for operations of the virtual machine. **(Altman- para. 28-32)**

Conclusion

27. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Ustaris can be reached on 571-272-7383. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2433
August 16, 2010